

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-172646
(43)Date of publication of application : 23.06.2000

(51)Int.Cl. G06F 15/00
G06F 9/06

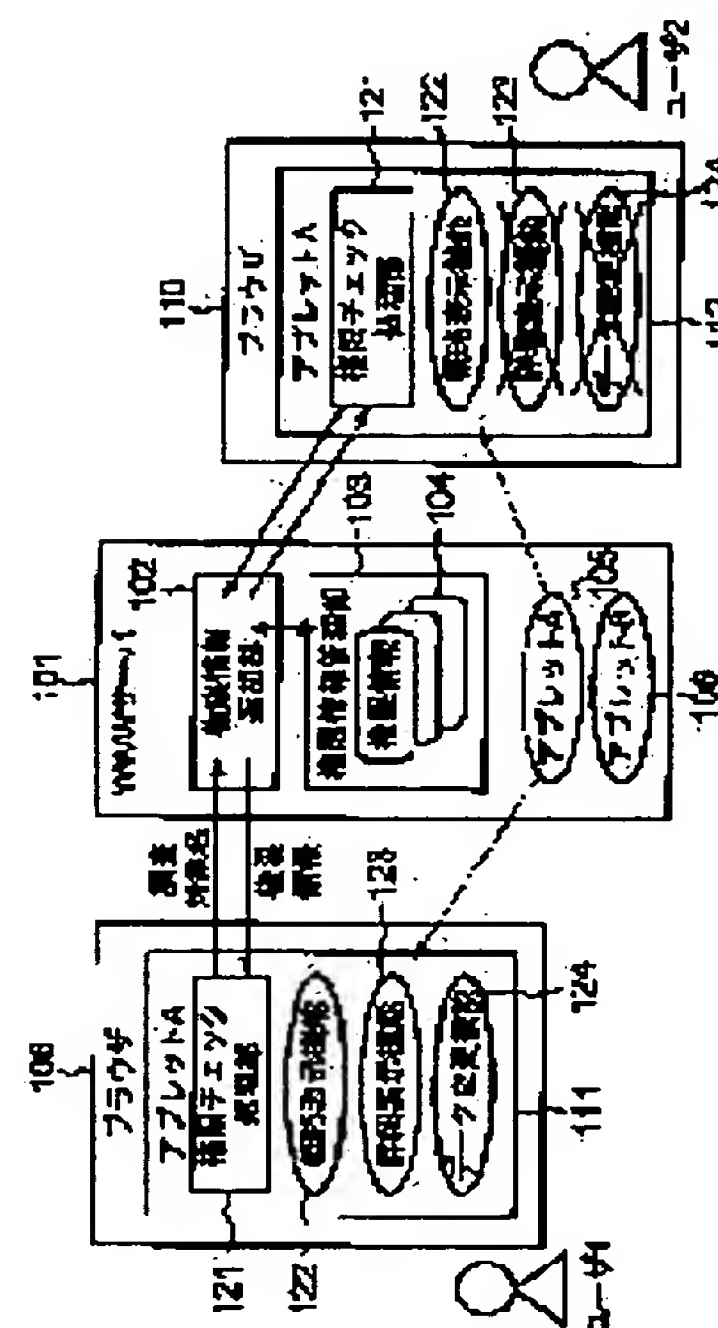
(21)Application number : 10-345635 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 04.12.1998 (72)Inventor : HASHIMOTO KEISUKE
HASEGAWA YOSHIRO

(54) APPLICATION FUNCTION DESIGNATING DEVICE AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To dynamically change execution enable or disable for part of function provided by an application at application execution with respect to the authority of a user, who executes that application, and to provide single sign on.

SOLUTION: This device is provided with authority information returning means 102 and 103 for returning authority information concerning the function, to which the execution is permitted to the user in response to demand from an application 111 for more than one function from among functions 122, 123 and 124 provided by that application corresponding to a request from that application.



LEGAL STATUS

[Date of request for examination] 06.02.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3563619
[Date of registration] 11.06.2004
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2000-172646

(P2000-172646A)

(43)公開日 平成12年6月23日(2000.6.23)

(51)Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 D 5 B 0 7 6
9/06	4 1 0	9/06	4 1 0 A 5 B 0 8 5
	5 5 0		5 5 0 G

審査請求 未請求 請求項の数 8 O L (全 15 頁)

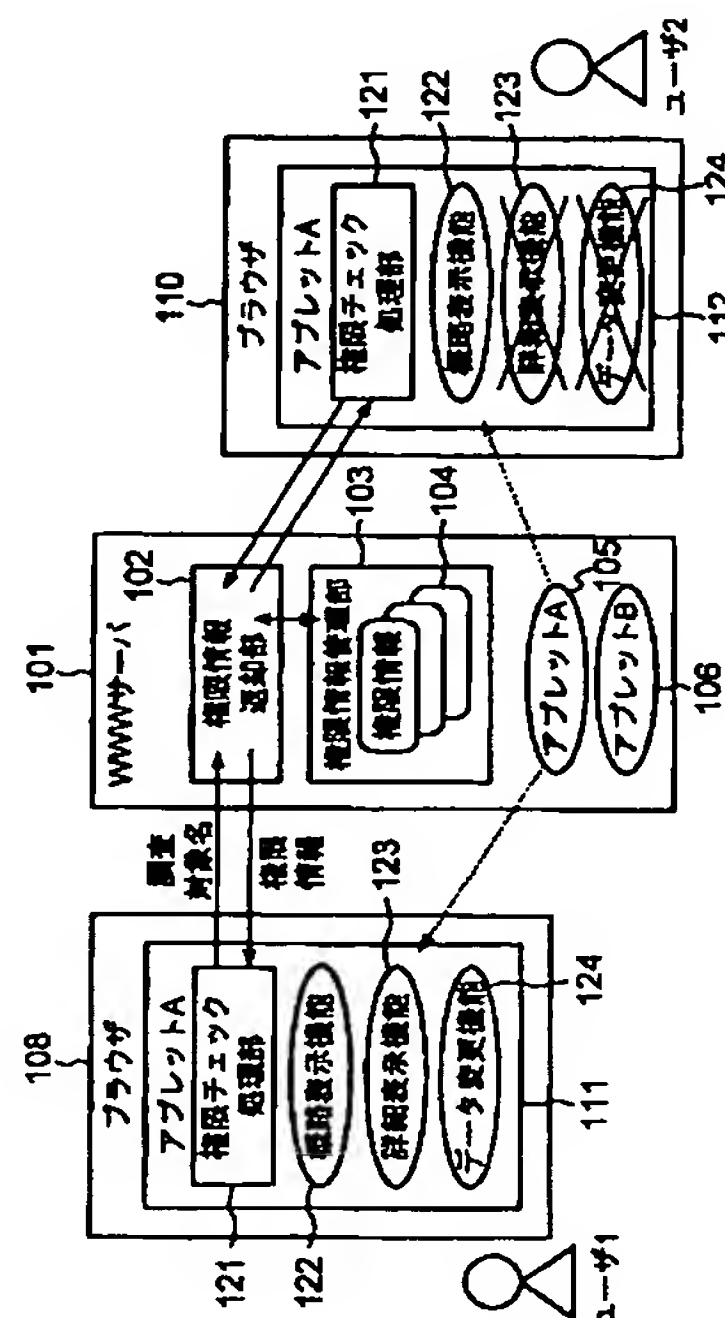
(21)出願番号	特願平10-345635	(71)出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22)出願日	平成10年12月4日(1998.12.4)	(72)発明者	橋本 圭介 東京都府中市東芝町1番地 株式会社東芝 府中工場内
		(72)発明者	長谷川 義朗 東京都府中市東芝町1番地 株式会社東芝 府中工場内
		(74)代理人	100058479 弁理士 鈴江 武彦 (外6名)
		Fターム(参考)	5B076 AB10 FB01 5B085 AE06 BE03 BG07

(54)【発明の名称】 アプリケーション機能指定装置及び記憶媒体

(57)【要約】

【課題】 アプリケーションを実行するユーザ権限に対応し、そのアプリケーションが提供する機能の一部を実行可能にしたり実行不可能にしたりすることをアプリケーション実行時に動的に変更でき、かつ、シングルサインオンを実現することができる。

【解決手段】 アプリケーション111からの要求に応じて、当該アプリケーションが提供する一以上の機能122、123、124のうち、当該アプリケーションを使用しているユーザに実行許可される機能についての権限情報125を返却する権限情報返却手段102、103を備えたことを特徴とするアプリケーション機能指定装置。



【特許請求の範囲】

【請求項1】 アプリケーションからの要求に応じて、当該アプリケーションが提供する一以上の機能のうち、当該アプリケーションを使用しているユーザに実行可否される機能についての権限情報を返却する権限情報返却手段を備えたことを特徴とするアプリケーション機能指定装置。

【請求項2】 アプリケーションからの権限情報要求に応じて、当該アプリケーションが有する一以上の機能のうち実行可能な機能を指定するアプリケーション機能指定装置であって、

各アプリケーションの有する各機能毎に実行可否され得るユーザの情報を実行権限情報として管理する権限情報管理手段と、

前記権限情報要求を出力したアプリケーションについての実行権限情報を前記権限情報管理手段から取得するとともに、当該実行権限情報に基づいて当該アプリケーションを使用しているユーザに実行可否される機能についての情報を作成しアプリケーションに返却する権限情報返却手段とを備えたことを特徴とするアプリケーション機能指定装置。

【請求項3】 WWWサーバ上に設けられた請求項2記載のアプリケーション機能指定装置であって、前記権限情報管理手段は、前記実行権限情報をWWWサーバで用いられるアクセスコントロールリストとして管理することを特徴とするアプリケーション機能指定装置。

【請求項4】 WWWサーバ上に設けられた請求項1乃至3のうち何れか1項記載のアプリケーション機能指定装置であって、前記権限情報返却手段は、WWWサーバの有するユーザ認証機構がユーザ認証したユーザを、前記アプリケーションを使用しているユーザとして特定することを特徴とするアプリケーション機能指定装置。

【請求項5】 アプリケーションからの要求に応じて、当該アプリケーションが提供する一以上の機能のうち、当該アプリケーションを使用しているユーザに実行可否される機能についての権限情報を返却させる権限情報返却手段を有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項6】 アプリケーションからの権限情報要求に応じて、当該アプリケーションが有する一以上の機能のうち実行可能な機能を指定するアプリケーション機能指定装置を制御するプログラムであって、各アプリケーションの有する各機能毎に実行可否され得るユーザの情報を実行権限情報として管理させる権限情報管理手段と、前記権限情報要求を出力したアプリケーションについての実行権限情報を前記権限情報管理手段から取得させるとともに、当該実行権限情報に基づいて当該アプリケー

ションを使用しているユーザに実行可否される機能についての情報を作成させアプリケーションに返却させる権限情報返却手段とを有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項7】 WWWサーバ上に設けられた請求項6記載のアプリケーション機能指定装置を制御するプログラムであって、

前記権限情報管理手段は、前記実行権限情報をWWWサーバで用いられるアクセスコントロールリストとして管理させることを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項8】 WWWサーバ上に設けられた請求項5乃至7のうち何れか1項記載のアプリケーション機能指定装置を制御するプログラムであって、前記権限情報返却手段は、WWWサーバの有するユーザ認証機構がユーザ認証させたユーザを、前記アプリケーションを使用しているユーザとして特定させることを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はアプリケーション機能指定装置及び記憶媒体、更に詳しくはWWWブラウザ上で動作するアプリケーションにおいて、アプリケーション実行者の権限によってそのアプリケーションで実行できる機能を動的に切り替えることを可能とするためのアプリケーション機能指定装置及び記憶媒体に関するものである。

【0002】

【従来の技術】近年のインターネット技術の発展に伴い、WWW（ワールドワイドウェブ）ブラウザ上で動作するJavaアプレット（以下、アプレットと記載）等のWWWアプリケーションが広く用いられるようになっている。

【0003】これらのアプリケーションには、その動作自体あるいは動作機能の一部にユーザに対応した使用制限が付されることも多い。例えばある一つのアプレットがいくつかの機能から構成されている場合を考える。このアプレットは、ユーザが持つ権限に応じてそれらの機能の一部を実行可能にしたり実行不可能にしたりを実行時に動的に変更する必要がある。この実行可能範囲の動的な変更機能を実現するため、従来から例えば次のような方法を取っている。

【0004】第1の方法は、アプレット自体がユーザ情報（ユーザ名・パスワードなど）を問い合わせるようにするものである。

【0005】すなわちアプレット実行時に、ユーザ（アプレット実行者）に対してユーザ情報（ユーザ名・パスワードなど）を入力させ、この情報をもとにアプレット内のどの機能を実行可能とし、どの機能を実行不可能にするかを決定するようにアプレットを作成する。

【0006】ただし、このためには、ユーザ認証機構や各ユーザユーザの権限情報を設定・管理する機構を別途作り込む必要がある。

【0007】第2の方法は、実行可能な機能の組み合わせごとに、別のアプレットをそれぞれ用意するものである。

【0008】例えば三つの機能A、B、Cをアプレットで実現する場合を考える。この場合には、

アプレット1：機能A、B、Cが実行可能なアプレット

アプレット2：機能A、Cが実行可能なアプレット

アプレット3：機能Aのみ実行可能なアプレット

という3種類のアプレットを用意し、それぞれに対してWWWサーバのアクセス制御機能に基づいたアクセス権の設定を行う。

【0009】すなわち、アプレット1は、機能A、B、Cすべてを実行可能なユーザにアクセス権を設定し、アプレット2は、機能AとCが実行可能なユーザにアクセス権を設定し、さらに、アプレット3は、機能Aのみ実行可能なユーザにアクセス権を設定するというものである。

【0010】これにより、例えば、機能Bを実行する権限のないユーザは、アプレット1をダウンロード・実行ができないことになる。

【0011】

【発明が解決しようとする課題】しかしながら、上記従来技術によってWWWアプリケーション機能の一部を実行時に動的変更する場合には、未だに解決すべき以下のような課題がある。

【0012】まず、アプレット自体がユーザ情報を問い合わせる上記第1の方法においては、そのアプレットに対して入力されるユーザ情報は、WWWブラウザ上で動作する当該アプレット内のみで有効な情報となる。

【0013】一方、WWWコンテンツに対するアクセス権が設定されている場合、WWWブラウザとWWWサーバの間でHTTPプロトコルを用いてユーザ情報が受け渡され、WWWサーバにおいてユーザ認証やアクセス権限の確認が行われる。

【0014】したがって、利用者は、アクセス権が設定されているWWWコンテンツにアクセスするときに、まずユーザ情報の入力を求められ、さらにこのアプレットを実行するときに再度ユーザ情報の入力を求められることになる。すなわち、シングルサインオン（一度の認証で複数のサービスを利用できる仕組み）が実現できないことになる。

【0015】また、この第1の方法では、ユーザ認証を行う機構やアクセス権限の管理・設定を行う機構をサーバ上に別途用意するか、アプレット内に含ませる必要がある。このような機構の実装に労力を要することになる。

【0016】さらに、ユーザ情報としてユーザ名とパス

ワードの組を使用する代わりに、電子証明書を使用することによりセキュリティレベルとユーザの利便性を向上させたい場合がある。この第1の方法に電子証明書を使用する方法を組み込むことを考えると、アプレットがユーザ情報を問い合わせるためには、電子証明書をその保管場所（WWWブラウザ、ICカードなど）から取り出す機構と、電子証明書の内容を解析してユーザ認証を行う機構を作り込む必要があり、実装のための労力が非常に大きくなる。

10 【0017】次に、実行可能な機能の組み合わせごとに別々のアプレットを用意する上記第2の方法においては、どのアプレットを実行するかは、メニューなどの形でユーザが選択することになる。しかし、その都度ユーザに選択させる形態を取るのが困難な場合がある。

20 【0018】例えば、アプレット1を実行した後にアプレット2を実行することにより作業が完遂するような処理を想定する。ここで、アプレット1が機能Aと機能Bからなっており、アプレット2が機能Cと機能Dからなっているとする。この場合、上記従来技術で述べた内容に従い、それぞれ次のような二つのアプレットとして実現することとする。

【0019】アプレット1a：機能A、Bが実行可能なアプレット1

アプレット1b：機能Aのみ実行可能なアプレット1

アプレット2a：機能C、Dが実行可能なアプレット2

アプレット2b：機能Cのみ実行可能なアプレット2

30 ここで、アプレットに1aに着目する。アプレット1aの処理終了後、アプレット2を呼び出すことになるが、アプレット2はアプレット2aと2bの二つのバリエーションがある。

【0020】一般にアプレット1aへのアクセス権を与えられているユーザがそのままアプレット2aへのアクセス権が与えられているとは限らないため、アプレット1aがアプレット2aを呼び出すかアプレット2bを呼び出すかは、アプレット1aの作成（実装）時には特定できない。このため、アプレット1aの実行時に次に呼出すアプレットを動的に変更する必要がある。

40 【0021】しかし、このような仕組みは提供されていないため、アプレット1a実行時に、ユーザに対してメニューなどの形により、アプレット2aを実行するかアプレット2bを実行するかの選択を行わせる必要がある。ところが現実には、アプレット1からアプレット2への処理の移行はユーザを介さず自動的に行ないたい場合が多いため、ユーザに対してその都度問い合わせを行うという形態にするのは困難な場合が多い。

50 【0022】また、一つのアプレットがたくさんの機能から構成されている場合、アプレット1a、1b、1c…というように多数のバリエーションのアプレットを作成することになり、実装および管理コストが非常に大きくなるという問題点もある。

【0023】本発明は、このような実情を考慮してなされたもので、アプリケーションを実行するユーザ権限に対応し、そのアプリケーションが提供する機能の一部を実行可能にしたり実行不可能にしたりすることをアプリケーション実行時に動的に変更でき、また、シングルサインオンを実現することができるアプリケーション機能指定装置及び記憶媒体を提供することを目的とする。

【0024】

【課題を解決するための手段】上記課題を解決するために、請求項1に対応する発明は、アプリケーションから10の要求に応じて、当該アプリケーションが提供する一以上の機能のうち、当該アプリケーションを使用しているユーザに実行可否される機能についての権限情報を返却する権限情報返却手段を有するアプリケーション機能指定装置である。

【0025】本発明はこのような手段を設けたので、アプリケーションを実行するユーザ権限に対応し、そのアプリケーションが提供する機能の一部を実行可能にしたり実行不可能にしたりすることができる。

【0026】次に、請求項2に対応する発明は、アプリケーションからの権限情報要求に応じて、当該アプリケーションが有する一以上の機能のうち実行可能な機能を指定するアプリケーション機能指定装置としてなされたものである。

【0027】このアプリケーション機能指定装置においては、権限情報管理手段によって、各アプリケーションの有する各機能毎に実行可否され得るユーザの情報が実行権限情報として管理されている。

【0028】また、権限情報返却手段によって、権限情報要求を出力したアプリケーションについての実行権限情報が権限情報管理手段から取得される。さらに、この実行権限情報に基づいて、アプリケーションを使用しているユーザに実行可否される機能についての情報が例えば実行可能機構一覧等の形で作成され、要求を行ったアプリケーションに返却される。

【0029】したがって、アプリケーションを実行するユーザ権限に対応し、そのアプリケーションが提供する機能の一部を実行可能にしたり実行不可能にしたりすることができる。

【0030】次に、請求項3に対応する発明は、WWWサーバ上に設けられた請求項2に対応する発明のアプリケーション機能指定装置についてなされたものである。

【0031】本発明においては、権限情報管理手段は、実行権限情報をWWWサーバで用いられるアクセスコントロールリストとして管理する。

【0032】したがって、本発明についてのシステム開発を容易かつ効率的に行うことができる。

【0033】次に、請求項4に対応する発明は、WWWサーバ上に設けられた請求項1～3に対応する発明のアプリケーション機能指定装置についてなされたものであ

る。

【0034】本発明の権限情報返却手段は、WWWサーバの有するユーザ認証機構の認証結果をそのまま利用することにより、アプリケーションの実行者を特定する。

【0035】したがって、WWWサーバのユーザ認証機構がシステム全体のユーザ認証を一括して行うことになるので、いわゆるシングルサインオンを実現させることができる。

【0036】次に、請求項5に対応する発明は、請求項1に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0037】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項1のアプリケーション機能指定装置として機能する。

【0038】次に、請求項6に対応する発明は、請求項2に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0039】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項2のアプリケーション機能指定装置として機能する。

【0040】次に、請求項7に対応する発明は、請求項3に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0041】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項3のアプリケーション機能指定装置として機能する。

【0042】次に、請求項8に対応する発明は、請求項4に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0043】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項4のアプリケーション機能指定装置として機能する。

【0044】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

（第1の実施形態）図1は本発明の第1の実施形態に係るアプリケーション機能指定装置を適用したネットワークシステムの構成例を示すブロック図である。

【0045】このネットワークシステムは、インターネットに接続される多数の計算機からなるものであり、何れかの計算機に各々設けられたWWWブラウザ108、110及びWWWサーバ101が同図に示されている。なお、計算機自体及び公衆回線等を用いたネットワーク網は図示を省略している。

【0046】WWWサーバ101は、一般的なWWWサーバ機能を有する他、権限情報返却部102と、権限情報管理部103とを備えている。さらにWWWサーバ101は、アプレット105とアプレット106を含む複数のアプレットを図示しない記憶手段に保持する。また権限情報管理部103は各アプレット105、106等

に対応した各権限情報104を管理する。

【0047】本実施形態のWWWアプリケーション機能指定装置は、WWWサーバ101上に権限情報返却部102及び権限情報管理部103が設けられることで実現されるものである。

【0048】また、図1に示す例では、ユーザ1がブラウザ108を、ユーザ2がブラウザ110を利用しており、WWWサーバ101上のアプレット105をそれぞれ自分のブラウザ上にダウンロードして実行している。各ブラウザ108、110上にダウンロードされ実行可能状態になったアプレットを、それぞれアプレット111、アプレット112とする。

【0049】権限情報返却部102は、アプレットからユーザ権限の問合せがあったときに、権限情報管理部103に対し当該ユーザがそのアプレットのどの機能を使用許可できるかについて問い合わせると共に、その問合せ結果に基づいて実行可能機能一覧を作成し当該一覧をアプレットに返す。この権限情報返却部102はアプレットから起動可能であれば特に実現方法は問わないが、具体的には例えばCGI(Common Gateway Interface)によって実行される形態、または、WWWサーバが公開しているWWWサーバの機能拡張用のAPI(アプリケーションインターフェース)を利用した形態等により実現可能である。

【0050】権限情報管理部103は、上記のように権限情報104を管理しており、権限情報返却部102から呼び出されると、指定されたアプレット及びユーザについての権限情報104の内容に対応した結果を返却する。なお、例えば権限情報返却部102がCGIによって実行される形態の場合には、権限情報返却部102から子プロセスとして起動される形態や、権限情報返却部102の中の一機能として同一プロセス内で実行される形態などが考えられる。

【0051】権限情報104は、WWWサーバ101が保持するアプレット毎に用意されるものであり、そのアプレットの各機能を何れのユーザが実行可能であることを示す情報である。

【0052】図2はアプレットAに対する権限情報の例を示す図である。

【0053】このアプレットA(105)は、このアプレット本来の処理機能として、概略表示機能122、詳細表示機能123、データ変更機能124を備えており、それぞれ同図に示すユーザが各機能の実行権限を有している。

【0054】アプレット105、106等は、上記アプレット本来の処理機能122、123、124等の他に、権限チェック処理部121を備えている。なお、アプレット本来の処理機能は、各アプレット毎に異なるものである。

【0055】権限チェック処理部121は、自己アプレ

ット名を添付してWWWサーバ101の権限情報返却部102を起動し、さらに同返却部102から実行可能機能一覧を受け取る。

【0056】また、権限チェック処理部121は、この実行可能機能一覧に基づき当該アプレットが有する各機能(アプレット本来の処理機能)のうち当該ユーザに実行許可されている機能を実行可能状態とする。なお、図1にはユーザ1、2に許可される機能が実行可能状態とされた例が示されている。

【0057】なお、WWWブラウザ108、110等は、ブラウザの標準機能として、WWWサーバ101からの要求に対応し、ユーザ識別情報(ユーザ名)及びパスワード等からなるユーザ情報を取得しサーバ101に送信する機能を有している(図示せず)。これにより、WWWサーバ101はWWWブラウザ108、110等の使用者をユーザ認証する。

【0058】次に、以上のように構成された本実施形態におけるアプリケーション機能指定装置の動作について説明する。

【0059】図3は本実施形態におけるWWWサーバ側の動作を示す流れ図である。

【0060】まず、アプレット111、112等から権限情報返却部102が呼び出され、調査対象アプレット名を受け取る(s1)。

【0061】次に、WWWサーバ101のサーバ機能によって、権限情報返却部102を呼び出したアプレットを実行しているユーザのユーザ名が権限情報返却部102に与えられる(s2)。ここで、ユーザ名の取り出しは、WWWサーバ101が標準で提供している機能を用いることにより実行可能である。

【0062】取得された調査対象アプレット名が引数として用いられ、権限情報返却部102により、権限情報管理部103に対する権限情報104の問い合わせが行われる(s3)。

【0063】ステップS303で受け取った調査対象アプレットに対する権限情報104が権限情報管理部103によって取り出され、権限情報返却部102に送信される(s4)。

【0064】この権限情報104は権限情報返却部102において解析され、ステップs2得た調査対象ユーザに実行権が与えられている機能の一覧(実行可能機能一覧)が作成される(s5)。

【0065】図4は実行可能機能一覧の内容例を示す図である。

【0066】あるユーザ1、2について、調査対象となるアプレットA、B等のもつ各機能に対し、実行が許可されているか許可されていないかの一覧が示されている。なお、同図に示す実行可能機能一覧125の例は、ユーザ2についてのアプレットAに関するものである。

【0067】この作成された実行可能機能一覧は、権限

10

20

30

40

50

情報返却部102によって呼び出し元のアプレット111、112等に返却される(s6)。

【0068】なお、上記ステップs5では、権限情報返却部102が、権限情報管理部103から受け取った情報と調査対象ユーザ名を突き合わせて実行可能機能一覧を生成するように記載したが、権限情報管理部103の呼び出し時に調査対象ユーザ名も引数として渡し、調査対象ユーザの実行可能機能一覧を権限情報管理部103が生成するような構成にしてもよい。

【0069】次に、権限情報返却部102から受け取った権限情報(実行可能機能一覧125)をもとに、与えられた権限に応じて動作を切り替えるべきアプレット111、112等の動作手順を、図5のフローチャートを用いて説明する。

【0070】図5は本実施形態におけるWWWブラウザ側の動作を示す流れ図である。

【0071】まず、ブラウザ108、110等においてアプレット111、112等の実行が開始されると(t1)、アプレット111、112等における権限チェック処理121によって、WWWサーバ101上の権限情報返却部102が起動される(t2)。

【0072】その後、権限情報返却部102が作成した実行可能機能一覧125が権限チェック処理部121に引き渡されると(t3)、当該一覧125に基づき、アプレットの有する機能のうち当該ユーザ1、2等に許される処理のみが権限チェック処理部121によって、又*

```
public void 詳細表示機能() {
    実行可能機能一覧を参照し、詳細表示機能の実行権が与えられているか
    調べる
    if (実行権限が与えられている) {
        詳細表示を行うルーチン
    }
}
```

このような形で、権限チェック処理部121、又はアプレット本来の処理機能122、123、124等を実行可能機能一覧125に基づく機能実行制限処理を作成しておくことにより、アプレット実行時に実行者の持つ権限に応じた動作切替えが実現される。

【0076】上述したように、本発明の実施の形態に係るアプリケーション機能指定装置は、WWWサーバ101に権限情報返却部102と権限情報管理部103を設け、アプレット111、112等からこれを利用するようにしたので、以下のような効果を得ることができる。

(1) アプレットの実行時に権限情報返却部102に依頼してユーザ権限を調べるようにしているので、ユーザ権限に応じ、実行可能な機能を実行時に動的に変更するアプレットを構成させることができる。

(2) したがって、提供する機能のうちどの機能を実行可能としてどの機能を実行不可能にするかを動的に変更可能となることから、異なるバリエーションのアプレッ

*はアプレット本来の処理機能122、123、124等自体が有する機能によって実行可能又は不可能状態となる。

【0073】なお、図1の例でアプレットAをユーザ2が使用する場合について説明すると、まず、アプレットAに対する権限情報は図2に示すとおりである。したがって、実行可能機能一覧125は図4に示す通りとなり、図1に示すように、「概略表示機能122」のみが実行可能状態となる。

【0074】ここで、アプレット111、112等が有する機能制御方法としては、例えば次のような方法が考えられる。

(1) アプレット使用者に権限が与えられていない機能を実行するようなGUI部品(ボタンなど)が権限チェック処理部121、又はアプレット本来の処理機能122、123、124等自体が有する機能によって、アプレットの実行画面作成時に表示しない、あるいは、該当GUI部品のプロパティを設定するなどにより、操作できない状態にされる。

(2) 実行可能機能一覧125をアプレット内に保持すると共に、アプレットの機能122等を提供する各メソッド内に、保持されている実行可能機能一覧を確認して権限が与えられていない場合はそのメソッドの実行を中止するようなルーチンを入れておく。例えば、以下ののような構成のメソッド定義となる。

【0075】

トをいくつも作成することが不要であり、実装および管理のコストを大幅に軽減させることができる。

(3) サーバ上に保持されている実行権限の情報をアプレット111、112等から参照する方式をとっているため、権限情報の設定・管理を効率的に行うことが可能であり、設定管理コストの軽減を図ることができる。また、権限情報を各クライアント側に持たせる(あるいは配布する)場合と異なり、権限情報の内容変更時の不整合が発生しない。

(4) また、ユーザ情報は、WWWサーバ101等を介して権限情報返却部102に引き渡されるので、WWWサーバ101のサーバ機能が有するユーザ認証機能をそのまま利用でき、この場合には再度ユーザ情報を要求する必要をなくし、いわゆるシングルサインオンを実現することができる。

【0077】なお、WWWサーバが標準で提供するユーザ認証機能は必ずしもそのまま利用する必要はなく、種

々の方法でユーザ名を取得することができる。

【0078】また、権限情報返却部102を例えばサーバ機能拡張用のAPIを用いて実現させたような場合においても、当該APIがWWWサーバ標準のユーザ認証機能を利用して、あるいは同ユーザ認証機能を利用せずに、ユーザ名の取得を行うようにすることができる。WWWサーバ標準のユーザ認証機能を利用しない場合には例えばアプレット111、112等の権限チェック処理部121にユーザ情報を送信させるようにしてもよい。

(第2の実施形態)本実施形態は、第1の実施形態における権限情報返却部102の実現方式として、CGIを用いた場合について説明する。

【0079】図6は本発明の第2の実施形態に係るアプリケーション機能指定装置を実現するWWWサーバの構成例を示すブロック図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0080】このWWWサーバ101は、権限情報返却部102がCGIプログラム(CGIによって実行されるプログラム)として構成されると共に、権限情報管理部103が権限情報返却部102の一機能として実現され同一プロセスとして動作する形態となっている他、第1の実施形態と同様に構成されている。なお、WWWサーバ101にはユーザ認証部131が設けられるが、同認証部131は一般的なWWWサーバ機能に標準的に含まれるものであって、第1の実施形態においてはその図示を省略している。

【0081】ユーザ認証部131は、アプレット111、112等から権限情報返却部102の実行要求を受けた場合等に、ユーザ認証を行うためにWWWブラウザ108、110等にユーザ情報を要求するとともに、自己が取得したあるいは既に取得しているユーザ情報を変数REMOTE_USERに設定する形で権限情報返却部102に付与する。

【0082】なお、CGIはWWWサーバ上でプログラムを実行させる仕組みであり、ブラウザ側から当該プログラムの実行を要求することでそのプログラム動作が実現される。

【0083】次に、以上のように構成された本実施形態におけるアプリケーション機能指定装置の動作について説明する。

【0084】図7は本実施形態におけるWWWアプリケーション機能指定装置の動作を示す流れ図である。

【0085】まず、アプレット111、112等の権限チェック処理部121からCGIにより権限情報返却部102に対する実行要求がなされる。このとき、CGIの引数として、権限情報調査対象名(アプレット名)が権限情報返却部102に渡される(u1)。

【0086】ここで、このアプレット111、112等の実行者がいまだにWWWサーバ101に対してユーザ

認証を行っていない場合には、ユーザ認証部131によってHTTPレベルでのユーザ情報送信がWWWブラウザ108、110等に対して要求される(ステップu2)。

【0087】これを受けてユーザに対してユーザ情報の入力を促す処理は、一般にWWWブラウザが標準で提供している機能(図示せず)であり、ポップアップウィンドウを表示してユーザにユーザ名とパスワードを入力させる形態が一般的である。また、該当WWWサーバに対するユーザ認証が既に行なわれている場合は、この時点でのこの処理は省かれる。

【0088】次に、WWWブラウザ108、110等からHTTP(Hyper Text Transfer Protocol)プロトコルを用いて送信されたユーザ情報がWWWサーバ101にて受信される(u3)。

【0089】ユーザ情報であるユーザ名とパスワードをもとに、WWWサーバ101のユーザ認証部131によってユーザ認証が行われ、認証された場合には、そのユーザ名がユーザ認証部131によって変数REMOTE_USERに設定される(u4)。この変数はCGIプログラムである権限情報返却部102から参照可能になっている。

【0090】次に、権限情報返却部102がCGIプログラムとして実行される(u5)。これによりまず、権限情報返却部102内で変数REMOTE_USERが参照されることにより、権限情報返却部102を起動したユーザ、すなわちアプレット111、112等を利用しているユーザのユーザ名が取得される。さらに、CGI起動時の引数が取り出されることにより、権限情報返却部102において、権限の調査対象名(アプレット名)が取得される(u6)。

【0091】次に、ステップu6で得られた調査対象名を引数として、権限情報管理部103(関数またはサブルーチン)に対して調査対象の権限情報の返却が要求される(u7)。

【0092】この調査対象名に基づき、権限情報管理部103によって当該調査対象の権限情報が検索され、その検索結果が権限情報返却部102に返却される(u8)。

【0093】ステップu6で得られたユーザ名と、ステップu8で得られた権限情報とが権限情報返却部102において突き合わされ、対象ユーザが実行可能な機能の一覧(実行可能機能一覧125)が作成される(u9)。

【0094】調査対象が「アプレットA」、対象ユーザが「ユーザ2」で、権限情報が図2のとおりである場合には、ユーザ2は「概略表示機能122」に対してのみ権限が与えられていることがわかるので、実行可能機能一覧125は図4に示したようになる。

【0095】ステップu9で得られた実行可能機能一覧125に基づいて権限情報返却部102によって返却値が構築され、さらにCGIの返却値としてアプレット111、112等に返却される(u10)。

【0096】なお、返却する情報(実行可能機能一覧125)のフォーマットとしては、例えば図8に示すような形式が考えられる。

【0097】図8は本実施形態におけるCGI返却値としての実行可能機能一覧の例を示す図である。

【0098】なお、ここでは権限情報返却部102が権限情報管理部103から受け取った情報と調査対象ユーザ名を突き合わせて実行可能機能一覧を生成するように記載したが、権限情報管理部103の呼び出し時に調査対象ユーザ名も引数として渡し、調査対象ユーザの実行可能機能一覧を権限情報管理部103が生成するような構成にしてもよい。

【0099】上述したように、本発明の実施の形態に係るアプリケーション機能指定装置は、権限情報返却部102をCGIとして構成させ、さらに権限情報管理部103も権限情報返却部102に連動するように構成させたので、以下のような効果を得ることができる。

(1) WWWサーバ、WWWブラウザが標準で提供しているユーザ認証機能をそのまま利用するため、これらの機能について新たな作り込みをする必要なく、システム構築の労力を低減させることができる。

(2) HTTPによるユーザ認証が行なわれるため、WWWブラウザから別のHTMLファイル等にアクセスする場合のユーザ認証との共通化を図ることができる。したがって、他のWWWシステムやWWWアプリケーションとの間で、シングルサインオンを容易に実現することができる。

(第3の実施形態) 第1及び第2の実施形態では、ユーザ認証に使用するユーザ情報として、ユーザ名とパスワードの組をユーザが入力する方式を用いたが、本実施形態ではユーザ情報として電子証明書を利用する場合を説明する。

【0100】本実施形態のアプリケーション機能指定装置は、ユーザ情報として電子証明書を用いる他、第1又は第2の実施形態と同様に構成されている。電子証明書とは、ユーザ名を含む情報に電子署名がなされたもの等である。

【0101】本実施形態におけるWWWブラウザ108、110等及びWWWサーバ101は、ユーザ認証を行うのに電子証明書を利用する機能を有する。なお、この機能は一般的なWWWブラウザ及びWWWサーバにて提供される標準的な機能である。

【0102】次に、以上のように構成された本実施形態におけるアプリケーション機能指定装置の動作について説明する。

【0103】この装置の動作は電子証明書を利用する以

外は第1又は第2の実施形態で述べた手順と同様である。

【0104】電子証明書については、まずWWWサーバ101により、HTTPプロトコルに従ったユーザ情報送信要求が送信される。

【0105】この要求を受信したWWWブラウザ108、110等においては、そのWWWブラウザ標準機能により、このブラウザ上で動作しているアプレット111、112等を使用しているユーザの電子証明書が取り出されWWWサーバ101に送信される。

【0106】このようにしてWWWサーバ101に送信された電子証明書は、そのWWWサーバ標準機能により解析され、ユーザ認証が行われる。

【0107】この結果、アプレット111、112等を使用しているユーザのユーザ名が第2の実施形態の場合と同様にして、CGIプログラムから参照可能な変数(REMOTE_USER)にセットされる。なお、権限情報返却部102等が、WWWサーバの機能を拡張するためのAPIによって構成される場合にも、当該APIの使用によりユーザ名を格納した変数を参照できるようになっている。

【0108】上述したように、本発明の実施の形態に係るアプリケーション機能指定装置は、ユーザ認証に電子証明書を利用できるようにしたので、以下のような効果を得ることができる。

(1) 電子証明書を利用することにより、セキュリティレベルの向上を図ることができる。

(2) 電子証明書を利用することにより、ブラウザ使用者は一々ユーザ名とパスワードの組を入力する必要がなく、ユーザの利便性を向上させることができる。

(3) 電子証明書を取り扱う機能はWWWブラウザおよびWWWサーバが標準で提供しているものをそのまま利用できるため、アプリケーション開発者などがこのような機能を作る込む必要がなく、アプリケーション開発を容易に行うことができる。

(第4の実施形態) 本実施形態では、第1～第3の実施形態における権限情報104を、その実施例として、図9に示すような形式のテキストファイルで実現する場合について説明する。

【0109】図9は本発明の第3の実施形態に係るアプリケーション機能指定装置における権限情報のデータ構造例を示す図である。

【0110】同図に示すように、この権限情報104は、レコードの区切りを空行とするデータ形式であり、一つのアプレットに対する権限の情報を1レコードで記述している。また、レコードの1行目に対象アプレット名を記述し、2行目移行にそのアプレットが提供するアクセス権を設定すべき機能名とその機能の実行を許可するユーザ名を記述する。

【0111】次に、以上のように構成された本実施形態

10

20

30

40

50

におけるアプリケーション機能指定装置の動作について図10のフローチャートを用いて説明する。

【0112】図10は本実施形態におけるWWWアプリケーション機能指定装置の動作を示す流れ図である。

【0113】まず、第1の実施形態の図3に示したステップs1、s2の処理については、本実施形態においても同様であるので説明を省略し、図3のステップs3～s6に対応する部分のみを説明する。なお、ここでは、権限情報の調査対象アプレット名が「アプレットA」であり、調査対象ユーザ名が「ユーザ2」として説明を行う。

【0114】まず、調査対象アプレット名（「アプレットA」）を引数として、権限情報返却部102によって権限情報管理部103に対する権限情報の問い合わせが行われる（v1）。

【0115】次に権限情報管理部103によって権限情報104が参照され、調査対象アプレット名に対応する権限情報、すなわちレコードの1行目に調査対象アプレット名が記述されているレコードの情報が抜き出される（v2）。

【0116】この例では調査対象アプレット名が「アプレットA」であるため、図9に示す権限情報のうち「アプレットA」に該当するレコードの内容、すなわち
対象：アプレットA

概略表示 ユーザ1、ユーザ2、ユーザ3、ユーザ4

詳細表示 ユーザ1、ユーザ4

データ変更 ユーザ1

が抜き出される。

【0117】次にステップv2で得られた権限情報が権限情報管理部103から権限情報返却部102に渡される（v3）。返却手段は、プロセス間通信、あるいは、ファイルや共有メモリによる受け渡し等の何れでもよく、特に手段は問わない。また、権限情報管理部103が権限情報返却部102の中の一機能として、同一プロセス内で実行される形態の場合は、構造体などのデータ構造の形で受け渡してもよい。

【0118】次に、ステップv3で受け取った権限情報は権限情報返却部102により参照され、各機能に設定された実行可能ユーザとして調査対象が含まれているかが調べられ、実行可能機能一覧125が作成される（v4）。

【0119】ここで、この例では調査対象ユーザが「ユーザ2」であるため、ステップv2で得た権限情報の各行に「ユーザ2」が含まれているかどうか調べられることにより、実行可能機能一覧125が作成される。

【0120】この場合、機能として「概略表示機能122」「詳細表示機能123」「データ変更機能124」の三つが記述されているが、ユーザ2は「概略表示機能122」の行にのみ権限有りとして記述されているため、実行可能機能一覧125は次のようになる。

【0121】概略表示OK

詳細表示NG

データ変更NG

実行可能機能一覧125の作成後、同一一覧125に対して、アプレット112に返却するために必要な情報が付加されて返却処理が実行される（v5）。なお、アプレット112との送受信をHTTPプロトコルを用いて行う場合、ここで付加する情報は「Content-Type: text/plain」ということになる。

【0122】なお、ここでは権限情報返却部102が、権限情報管理部103から受け取った情報と調査対象ユーザ名を突き合わせて実行可能機能一覧を生成するように記載したが、権限情報管理部103の呼び出し時に調査対象ユーザ名も引数として渡し、調査対象ユーザの実行可能機能一覧を権限情報管理部103が生成するような構成にしてもよい。

【0123】上述したように、本発明の実施の形態に係るアプリケーション機能指定装置は、レコードの区切りを空行とするデータ形式で権限情報104を記述するようにしたので、上記各実施形態における作用効果を容易に実現させることができる。

（第5の実施形態）本実施形態では、第1～第4実施形態における権限情報管理部103を、権限情報104をアクセスコントロールリスト（ACL: Access Control List）の形態で提供することにより実現する場合を説明する。

【0124】図11は本発明の第5の実施形態に係るアプリケーション機能指定装置を適用したWWWサーバの構成例を示すブロック図であり、図1～図10と同一部分には同一符号を付してその説明を省略する。

【0125】このWWWアプリケーション機能指定装置は、権限情報管理部103が問合せ管理部151、ACL管理部152及びACL格納部153から構成される他、第1～第4の実施形態と同様に構成されている。

【0126】ここで、ACL管理部152は、ACLの設定・管理、および、ACLの解析を行い設定内容を返却する機能を提供するもので、WWWサーバが標準で提供する機能をそのまま使用する。

【0127】なお、一般的なWWWサーバは、ACL管理部152の機能を利用して、ACLの設定・管理を行うためのユーザインタフェースを提供している。また、ACL管理部152の機能を利用するためのAPIを公開している場合もある。ユーザインタフェースやAPIを提供していないWWWサーバの場合は、ACL設定・管理機能をCGIプログラムなどの形で実装することにより、ACL管理部152を構成する。

【0128】ACL格納部153は、一つのコンテンツ（ファイル）に対するアクセス権の設定情報からなるACE（Access Control Entry）154が複数集まってなるACLを格納する。なお、AC

Lの取り扱い機能自体もWWWサーバが提供する標準機能である。

【0129】図12はACEの一例を示す図である。

【0130】同図に示すACEの例では、sample.htmlというコンテンツに対してユーザ1とユーザ2にread権限を与えている様子が示されている。ACLやその構成要素であるACEの記述フォーマットはWWWサーバ毎に異なっているが、ここに含まれる情報は基本的にはすべて同等なものである。

【0131】次に、問合せ管理部151は、情報交換部155とACL管理部152に対するインターフェースとしてのACL問合せ部156とを備える。

【0132】この問合せ管理部151は、権限情報返却部102から与えられたアプレット名等の情報を、ACL管理部152で用いられる形式の命令に変換して、ACL管理部152に対してACEを要求する。また、ACL管理部152から受け取った情報を権限情報返却部102に返す。

【0133】ここで、情報交換部155は、権限情報返却部102から与えられたアプレット名等の情報を、ACL管理部152で用いられる形式の命令に変換するものであり、この変換のために、例えば図13に示すようなテーブルを備えている。

【0134】図13は本実施形態における情報交換部155が有する情報交換テーブルの一例を示す図である。

【0135】同図に示すように、このテーブルでは、例えばあるアプレット名を受け取ると、当該情報を対応するACEからアプレット情報を取得するコマンドに変換するようになっている。

【0136】次に、以上のように構成された本実施形態におけるアプリケーション機能指定装置の動作について説明する。

【0137】まず、WWWアプリケーション機能指定装置の具体的な動作説明に先立って、権限情報104をACLとして設定する手順を説明する。権限情報104の例として第1の実施形態における図2に例示した情報を使用する。

【0138】まず、権限情報を設定するために、いくつかのファイルを作成する。ここでは一例として、ファイル名の命名規則を「対象名.機能名.ac1」とする。この命名規則は一例であり、以下に述べるような処理が行なえる形であれば他の形態でもよい。

【0139】図2に示したように、アプレットAは三つの機能から構成されているため、上記命名規則に従うと、「アプレットA.概略表示.ac1」「アプレットA.詳細表示.ac1」「アプレットA.データ変更.ac1」という名前のファイルを生成することになる。

【0140】次に、WWWサーバ101が提供するインターフェースを使用する等により、上記三つのファイルに対してACLの設定を行う。設定方法は通常のHTML

Lファイル等に対して設定する場合と同様である。

【0141】図2によると、アプレットAの概略表示機能は、ユーザ1、ユーザ2、ユーザ3、ユーザ4が実行権限を持っているため、「アプレットA.概略表示.ac1」というファイルに対して、これら4ユーザに対してアクセス権を与えるようにACLを設定する。以下同様にして設定したACLの例を、図14に示す。

【0142】図14は本実施形態におけるACLの一例を示す図である。

【0143】次に、WWWアプリケーション機能指定装置の具体的な動作説明を行う。

【0144】本実施形態において、先の実施形態と同様な動作部分については省略し、以下、第1実施形態の図3におけるステップs3以降について、すなわち権限情報返却部102からの要求で権限情報管理部103が権限情報を取り出して返却するまでについて説明する。ここでは権限情報の調査対象が「アプレットA」とする。

【0145】まず、権限情報返却部102から権限情報管理部103の問合せ管理部151に対し、アプレットAについての権限情報が要求される。問合せ管理部151ではアプレット名（アプレットA）が情報交換テーブルによりACL管理部152へのコマンドに変換され、同コマンドによってACL管理部152に対して、アプレットAの各機能に対する権限情報を設定したACE群を返却するように要求される。

【0146】次に、ACL管理部152によりACLが解析され、対象となるACE群が取り出されて、問合せ管理部151に返却される。対象となるACE群とは、具体的には「path="アプレットA.*.ac1"」となっている（"＊"は任意の文字列を表わすワイルドカード）ACEということになる。この例では、図14に示した三つのACEが対応する。

【0147】ACL管理部152から受け取ったACE群は、問合せ管理部151によって権限情報返却部102に送信される。この時、受け取ったACE群をそのまま送信してもよいし、権限情報返却部102が扱いやすいようにフォーマットを変換してもよい。例えば以下のように、ACE一つの情報を1行にまとめる等の処理を行ってもよい。

【0148】

概略表示	ユーザ1, ユーザ2, ユーザ3, ユーザ4
詳細表示	ユーザ1, ユーザ4
データ変更	ユーザ1

その他、権限情報返却部102と権限情報管理部103が同一プロセスとして動作する形態の場合であれば、構造体などのデータ構造の形で受け渡してもよい。

【0149】権限情報管理部103から受け取った権限情報は権限情報返却部102によって参照され、各機能に設定された実行可能ユーザとして調査対象ユーザが含

まれているかが調べられる。この調査結果に基づいて、アプレットに対して返却するデータ形式が作成される。

【0150】ここで、調査対象ユーザが「ユーザ2」であるとする、「ユーザ2」は「概略表示」の実行可能ユーザにのみ含まれているため、次のような実行可能機能一覧が作成される。

【0151】概略表示OK

詳細表示NG

データ変更NG

そして、この実行可能機能一覧125に対し、アプレット112に返却するために必要な情報が付加され同アプレット112に返却される。アプレットとの送受信をHTTPプロトコルを用いて行う場合、ここで付加する情報は「Content-Type: text/plain」ということになる。

【0152】なお、ここでは権限情報返却部102が、権限情報管理部103から受け取った情報と調査対象ユーザ名を突き合わせて実行可能機能一覧を生成するように記載したが、権限情報管理部103の呼び出し時に調査対象ユーザ名も引数として渡し、調査対象ユーザの実行可能機能一覧を権限情報管理部103が生成するような構成にしてもよい。

【0153】上述したように、本発明の実施の形態に係るアプリケーション機能指定装置は、権限情報104を、ACLを利用して設定することで権限情報管理部103を実現するようにしたので、ACLの設定・管理や設定内容の解析にWWWサーバが標準で提供する機能(API)やユーザインタフェースを利用することができ、システム開発労力を低減させることができる。

【0154】

【実施例】第1～第5の実施形態にかかるアプリケーション機能指定装置及びWWWアプリケーション(アプレット)を利用した実施例について説明する。ここではアプレット111、112等の持つ各機能122等に対する権限情報104をもとに、アプレットの機能を動的に変更するようなアプリケーションの一例を説明する。本実施例で想定するアプリケーションは、次のようなものである。

(1) 機器構成図をHTMLとして表示する。

(2) 設定を行ないたい機器をクリックすることにより、その機器の設定を変更するアプレットが起動される。

(3) 設定を変更する権限を持つユーザが実行した場合、このアプレットは設定の変更を行う機能を提供しているものとなり、設定を変更する権限を持たないユーザが実行した場合は、現在の設定値を表示するだけの機能を提供するものとなる。

【0155】図15は本発明の実施例におけるアプリケーションが表示する機器構成図の一例を示す図である。

【0156】この機器構成図は一つのHTMLファイル

で構成されており、機器A、機器B、機器Cの部分がクリッカブルマップ等のHTMLの機能を利用して、それぞれの設定を変更する機能を提供するアプレットが実行されるようにリンクが張られている。

【0157】このようにして実行されるアプレットの画面例を図16、図17に示す。

【0158】図16は設定変更権限を持たないユーザが実行した場合の画面例を示す図である。

【0159】図17は設定変更権限を持ったユーザが実行した場合の画面例を示す図である。同図に示す例では、値を表示しているフィールドが編集可能になっていて、「設定変更」ボタンが設置されている。

【0160】次にWWWアプリケーション機能指定装置及びアプリケーションの動作を説明する。まず、機器の設定を変更するアプレット側の処理手順を説明する。このアプレットは次のような流れで動作する。

【0161】まず、WWWサーバ101の権限情報返却部102に対して実行可能機能一覧125が要求される。

【0162】権限情報返却部102から、このアプレットを実行しているユーザの実行可能機能一覧を受け取る。

【0163】一方、初期画面として、「対象」「管理者」などのラベルと、設定値を表示するフィールドがアプレットの機能により設置される。

【0164】受け取った実行可能機能一覧が確認され、設定変更権限を持ったユーザかどうか調べられる。この調査は、各機能に埋め込まれた処理により行われてもよく、また権限チェック処理部121により行われてもよい。

【0165】ここで、設定変更権限を持ったユーザの場合、設定値表示フィールドが変更可能に設定され、図17に示すように設定変更ボタンが設置される。

【0166】次に、対象機器から現在の設定値が取得され、図16、図17に示す各フィールドに値が表示される。

【0167】また、図17に示す設定変更ボタンが押された場合には、各フィールドの値が取り出され、使用者の入力に応じて対象機器の設定が変更される。

【0168】以上がアプリケーションにおける処理である。次に、図15の機器構成図について説明する。

【0169】これは、クリッカブルマップなどの機能を用いて作成されている一つのHTMLであり、例えば「機器A」の部分をクリックすると、機器Aの設定を変更するアプレットが起動される。ここで、機器Aの設定を変更するアプレットを起動するように設定したHTMLファイルを「機器A.html」と仮定すると、機器構成図の「機器A」の部分から「機器A.html」へリンクを張ることになる。

【0170】ここで本実施例では、権限情報返却部10

2に対して実行可能機能一覧125を問い合わせるようにし、機器の設定を変更するアプレットを構築しているので、アプレットの実態は一つだけである。したがって、「機器構成図」は一種類だけ用意すればよい。

【0171】これに対し、実施例との比較のため、機器Aの設定を変更するアプレットを、従来技術で述べたように機能ごとに別のアプレットとして実装する場合を考える。すなわち、設定情報を表示するだけの機能を持つ「アプレットA1」と、表示および設定変更機能を持つ「アプレットA2」の二つのアプレットが作られる。機器構成図の「機器A」の部分からのリンク先は、HTMLの制約から一つのリンク先しか設定できないため、このような構成の場合、「設定変更を行う権限を持たないユーザ用の機器構成図」と「設定変更を行う権限を持つユーザ用の機器構成図」の二つを用意する必要がある。前者はアプレットA1を起動するように設定されており、後者はアプレットA2を起動するように設定されている。

【0172】更に機器Bについて従来技術を用いた場合を考える。あるユーザが機器Aに対して持っている権限と機器Bに対して持っている権限は、一般には一致しないことが想定される。すなわち、機器Aに対しては設定変更権限を持つが、機器Bに対しては設定変更権限を与えられていないユーザの存在が想定される。したがって、「機器構成図」として、「機器A、Bともに設定変更を行なえるユーザ用の機器構成図」「機器Aのみ設定変更を行なえるユーザ用の機器構成図」「機器Bのみ設定変更を行なえるユーザ用の機器構成図」「機器A、Bとも設定変更を行なえないユーザ用の機器構成図」の4通りを用意する必要がある。さらに機器数が増加すると、用意する「機器構成図」の種類が組み合わせ的爆発を起こすことになる。

【0173】しかし、上述したように本実施例のWWWアプリケーション機能指定装置によれば、権限情報返却部102に対して実行可能機能一覧125を問い合わせるようにして機器の設定を変更できるアプレットが用いられるので、アプレットの実態を一つだけにすることができ、「機器構成図」は一種類だけ用意すればよい。

【0174】なお、本発明は、上記各実施形態及び実施例に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【0175】例えば各実施形態で権限情報返却部102は、ブラウザ（アプレット）に対し機能の実行可否リストを実行可能機能一覧という形で返却するようにしたが、本発明は、実行可能情報を返却するという形態に限られるものではない。例えば実行拒否する機能についての情報を返却するようにしたり、実行許可、実況許可、条件付きで実行許可等といった情報を返却するようにしても良い。

【0176】また、本発明が適用される状況はネットワ

ークを介して実行可否を求める場合に限られない。例えば一計算機内のアプリケーションが当該計算機内の他のプログラム（アプリケーション機能指定装置に相当）に対し、自己が多数有する機能のうち実行許可される機能を問合せるような場合にも適用できる。

【0177】また、実施形態及び実施例に説明した装置は、記憶媒体に格納したプログラムをコンピュータに読み込ませることで実現させることができる。

【0178】ここで本発明における記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD等）、光磁気ディスク（MO等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【0179】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【0180】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【0181】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。

【0182】なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【0183】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0184】

【発明の効果】以上詳記したように本発明によれば、各アプリケーション及び各ユーザについての権限情報を管理するとともに、アプリケーションの権限チェック要求に応じて動作可能な機能の情報を返すようにしたので、アプリケーションを実行するユーザ権限に対応し、そのアプリケーションが提供する機能の一部を実行可能にしたり実行不可能にしたりすることをアプリケーション実行時に動的に変更できるアプリケーション機能指定装置及び記憶媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るアプリケーショ

ン機能指定装置を適用したネットワークシステムの構成例を示すブロック図。

【図2】アプレットAに対する権限情報の例を示す図。

【図3】同実施形態におけるWWWサーバ側の動作を示す流れ図。

【図4】実行可能機能一覧の内容例を示す図。

【図5】同実施形態におけるWWWブラウザ側の動作を示す流れ図。

【図6】本発明の第2の実施形態に係るアプリケーション機能指定装置を実現するWWWサーバの構成例を示すブロック図。

【図7】同実施形態におけるアプリケーション機能指定装置の動作を示す流れ図。

【図8】同実施形態におけるCGI返却値としての実行可能機能一覧の例を示す図。

【図9】本発明の第3の実施形態に係るアプリケーション機能指定装置における権限情報のデータ構造例を示す図。

【図10】同実施形態におけるアプリケーション機能指定装置の動作を示す流れ図。

【図11】本発明の第5の実施形態に係るアプリケーション機能指定装置を適用したWWWサーバの構成例を示すブロック図。

【図12】ACEの一例を示す図。

【図13】同実施形態における情報交換部155が有する情報交換テーブルの一例を示す図。

【図14】同実施形態におけるACLの一例を示す図。

【図15】本発明の実施例におけるアプリケーションが表示する機器構成図の一例を示す図。

【図16】設定変更権限を持たないユーザが実行した場合の画面例を示す図。

*【図17】設定変更権限を持ったユーザが実行した場合の画面例を示す図。

【符号の説明】

101…WWWサーバ

102…権限情報返却部

103…権限情報管理部

104…権限情報

105…サーバ上に保持されているアプレット

106…サーバ上に保持されているアプレット

107…ユーザ

108…ブラウザ

109…ユーザ

110…ブラウザ

111…ブラウザ上にダウンロードされて実行されているアプレット

112…ブラウザ上にダウンロードされて実行されているアプレット

121…権限チェック処理部

122…概略表示機能

123…詳細表示機能

124…データ変更機能

125…実行可能機能一覧

131…WWWサーバのユーザ認証部

132…変数

151…問合せ管理部

152…ACL管理部

153…ACL格納部

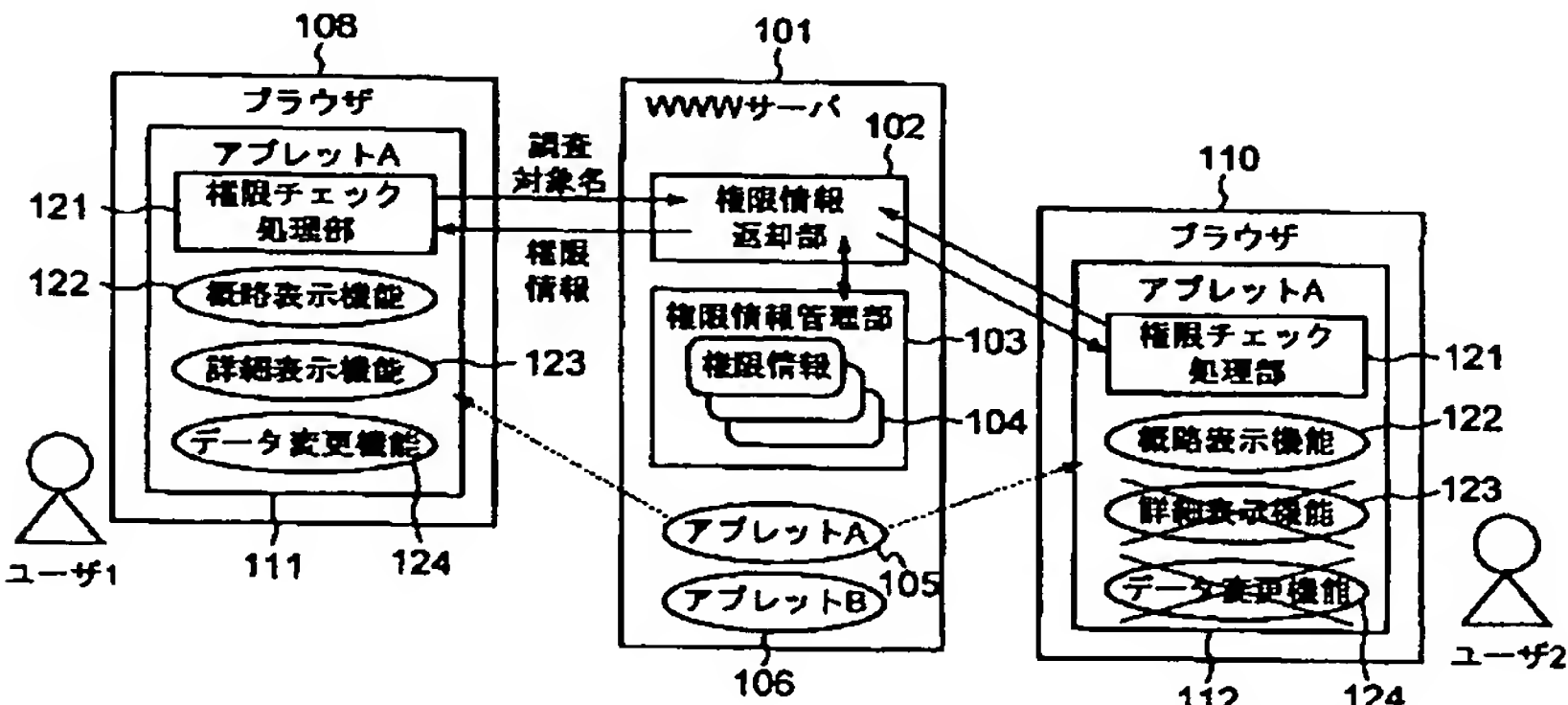
154…ACE

155…情報交換部

156…ACL問合せ部

*

【図1】



【図4】

125	
概略表示	OK
詳細表示	NG
データ変更	NG

【図8】

Content-Type : text/plain	
概略表示OK	
詳細表示NG	
データ変更NG	

【図2】

対象：アプレットA	
機能	実行可能者
概略表示	ユーザ1, ユーザ2, ユーザ3, ユーザ4
詳細表示	ユーザ1, ユーザ4
データ変更	ユーザ1

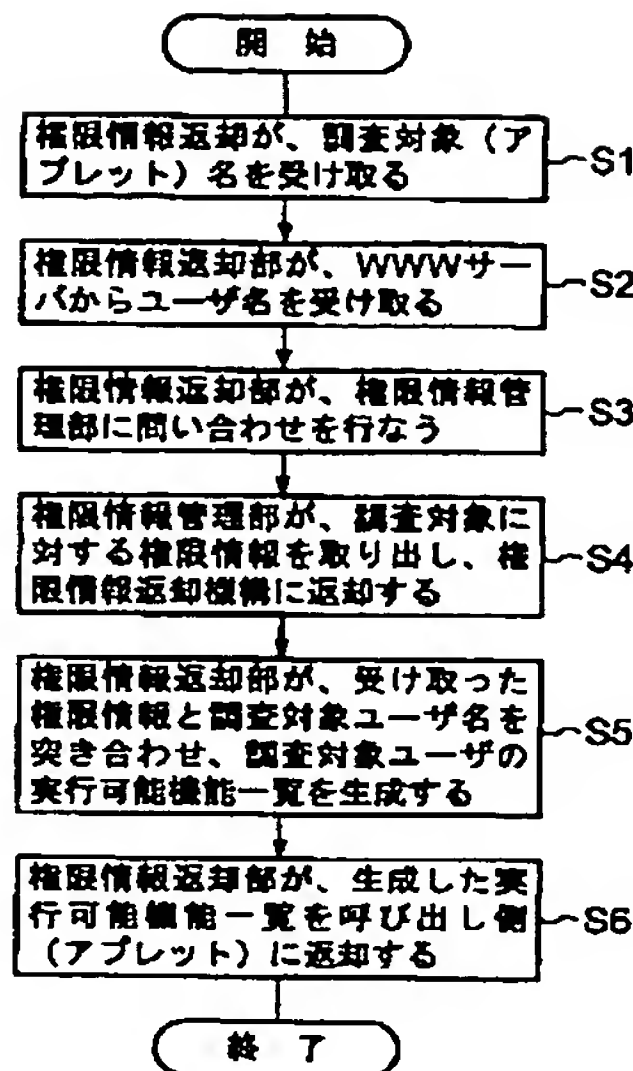
【図14】

path="アプレットA.概略表示.aci"
allow(execute)
user="ユーザ1, ユーザ2, ユーザ3, ユーザ4"

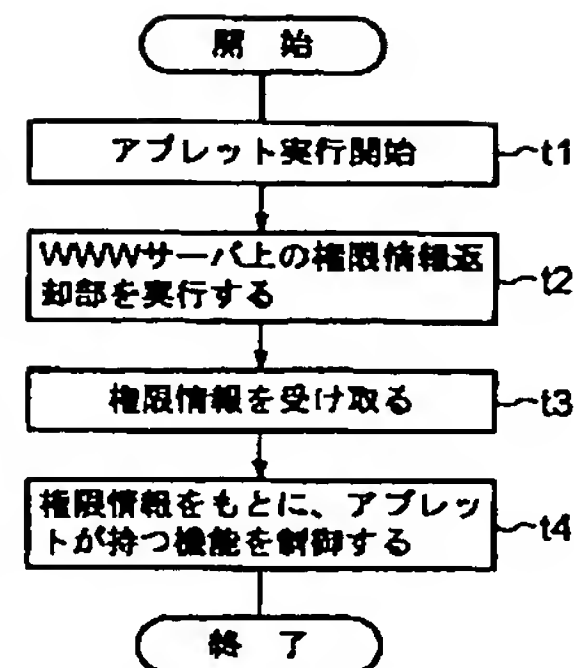
path="アプレットA.詳細表示.aci"
allow(execute)
user="ユーザ1, ユーザ4"

path="アプレットA.データ変更.aci"
allow(execute)
user="ユーザ1"

【図3】



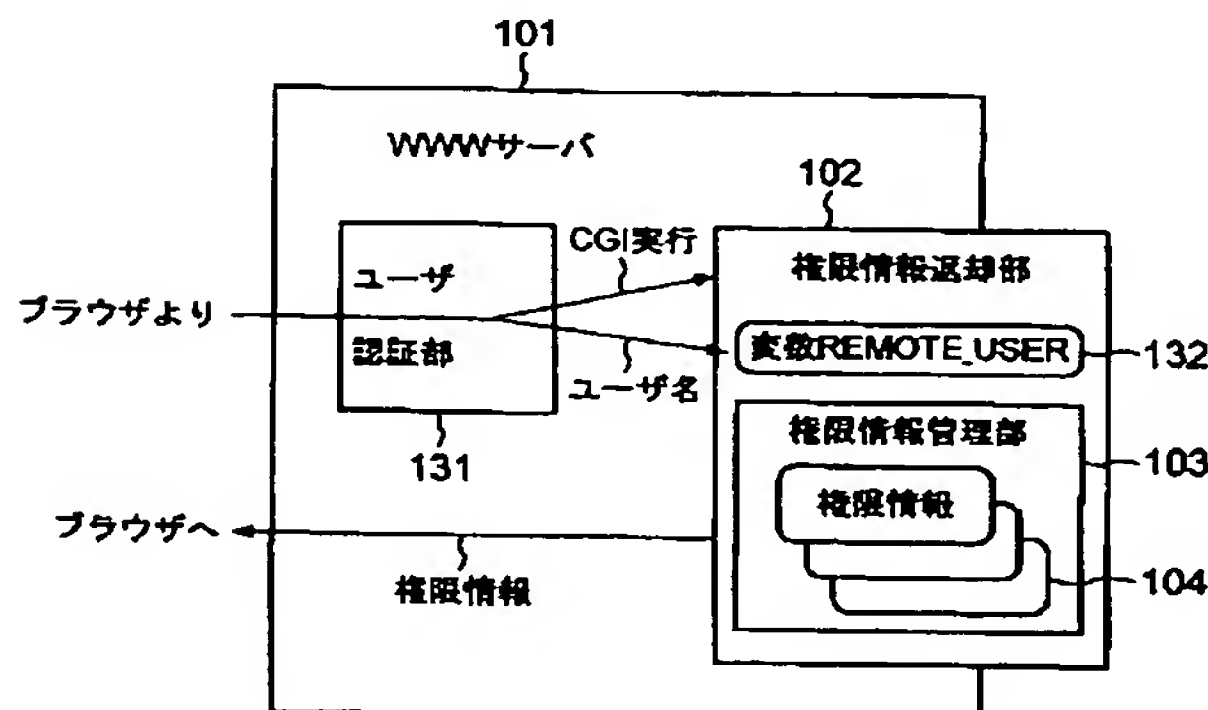
【図5】



【図12】

path="sample.html"
allow(read)
user="ユーザ1, ユーザ2"

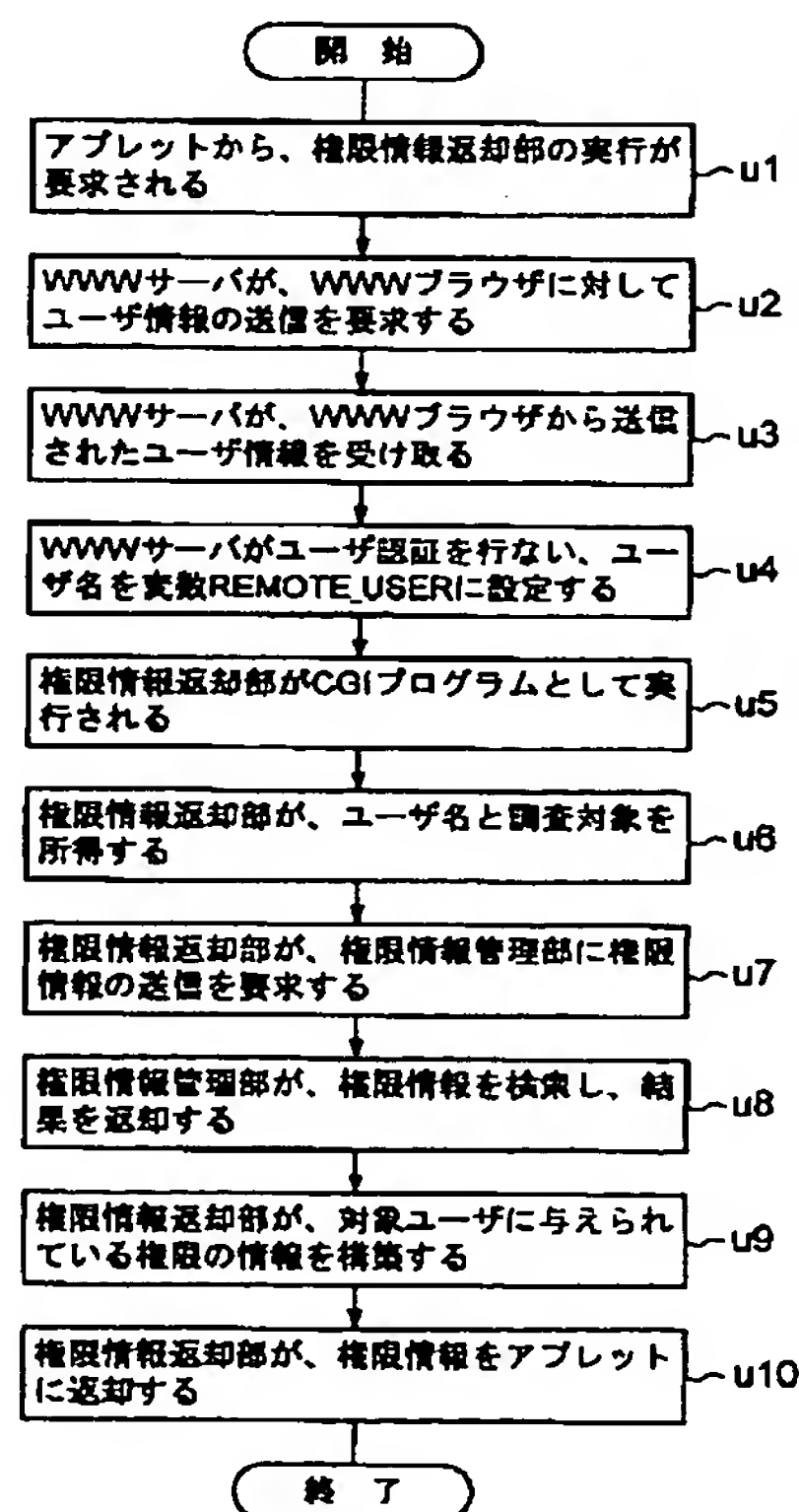
【図6】



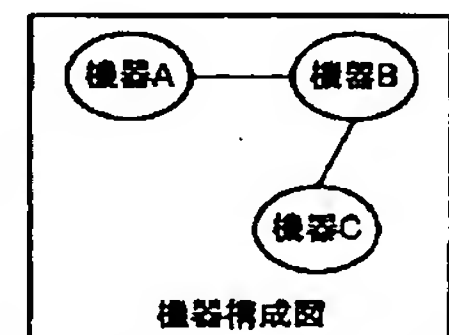
【図9】

対象：アプレットA	
概略表示	ユーザ1, ユーザ2, ユーザ3, ユーザ4
詳細表示	ユーザ1, ユーザ4
データ変更	ユーザ1
対象：アプレットB	
申請一覧表示	ユーザ1, ユーザ2
承認処理	ユーザ1

【図7】



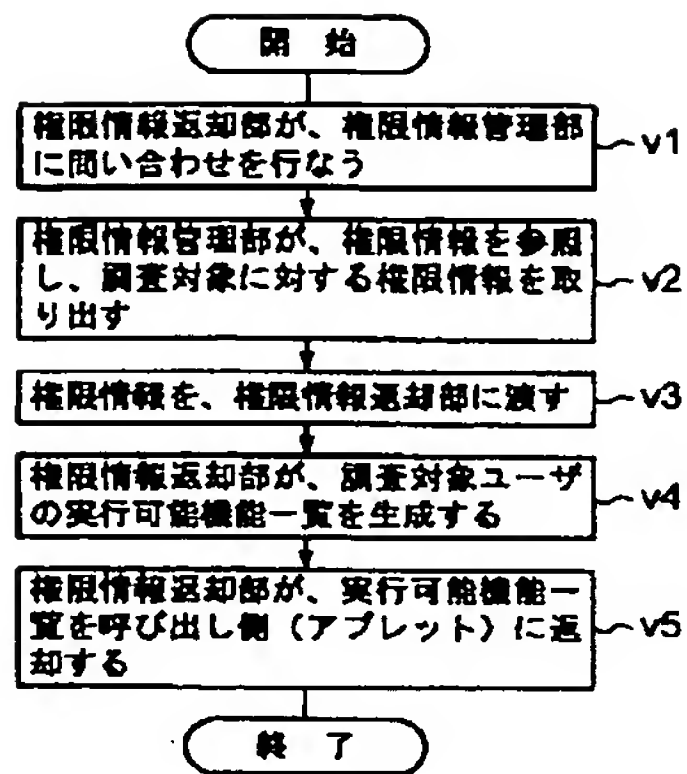
【図15】



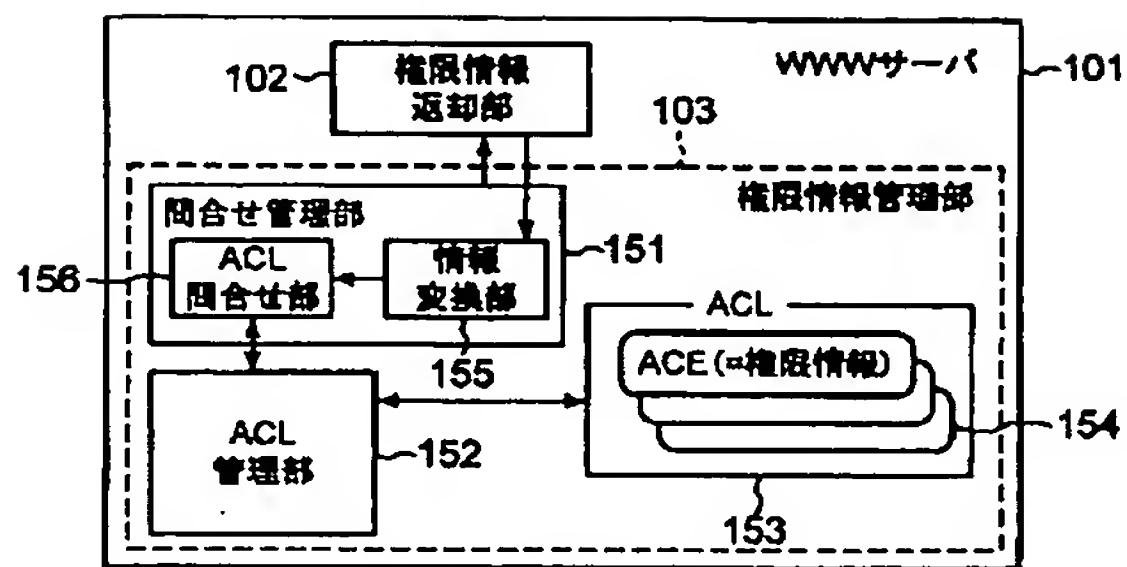
【図16】

対象	機器A
管理者	田中
設定値x	100
設定値y	50

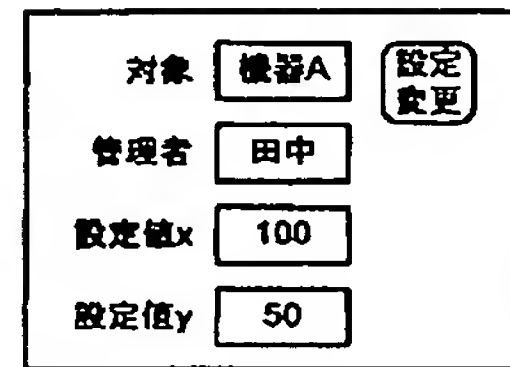
【図10】



【図11】



【図17】



【図13】

入力	ACL管理部への出力
アプレット名	get ACE (アプレット名)
アプレット名, ユーザ名	get ACE (アプレット名, ユーザ名)
⋮	⋮